

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
МБДОУ «Детский сад № 8»
г. Кольчугино

ПРИНЯТО
общим собранием работников
протокол № 1 от 30.08.2023

Мнение совета родителей
(законных представителей)

УЧТЕНО:

Председатель совета родителей
(законных представителей)

_____ Галкина О.С.

УТВЕРЖДАЮ
Заведующий МБДОУ «Детский сад № 8»
_____ Н.М. Малова
Приказ № 51 от 09.09.2023

ПОЛИТИКА
МБДОУ «ДЕТСКИЙ САД № 8»
В ОТНОШЕНИИ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ

2023 год

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика МБДОУ «ДЕТСКИЙ САД № 8» (далее соответственно – Политика, Учреждение) в отношении обработки персональных данных разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает Учреждение (далее – Оператор).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на официальном сайте Оператора.

1.5. Основные понятия, используемые в Политике:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Законом о персональных данных;

оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1.6. Основные права и обязанности Оператора.

1.6.1. Оператор имеет право:

1) самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

2) поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

3) в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных;

4) отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным Законом о персональных данных. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе;

5) осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных;

- включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- в случае, если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;
- обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

1.6.2. Оператор обязан:

- 1) организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;
- 2) отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;
- 3) сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;
- 4) обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- 5) в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения;
- 6) обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им персональных данных, в случае принятия Роскомнадзором решения о запрещении или об ограничении трансграничной передачи персональных данных;
- 7) немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- 8) разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;
- 9) предоставить субъекту персональных данных по его просьбе информацию, предусмотренную Законом о персональных данных;
- 10) разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку;
- 11) обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных;
- 12) в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие

с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных;

13) принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами;

14) опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

15) представить документы и локальные акты, указанные в Законе о персональных данных, и (или) иным образом подтвердить принятие мер, предусмотренных Законом о персональных данных, по запросу уполномоченного органа по защите прав субъектов персональных данных.

1.7. Основные права субъекта персональных данных.

Субъект персональных данных имеет право:

1) получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

2) требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных;

4) на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.8. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора.

1.9. Ответственность за нарушение требований законодательства Российской Федерации и локальных актов Учреждения в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

II. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.3. Обработка Оператором персональных данных осуществляется в следующих целях:

1. Цель обработки: подбор персонала (соискателей) на вакантные должности Оператора		
Категории данных	Персональные данные	Специальные данные
Перечень	фамилия, имя, отчество;	сведения о состоянии здоровья

данных	пол; гражданство; год рождения; месяц рождения; дата рождения; место рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; СНИЛС; ИНН; сведения об образовании; сведения о квалификации; сведения о профессиональной подготовке и повышении квалификации; семейное положение; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; иные персональные данные, предоставляемые соискателями по их желанию	сведения о судимости	
Категории субъектов	Кандидаты на работу (соискатели)		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока, необходимого для рассмотрения кандидатуры соискателя и заключения трудового договора		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе для анкеты (резюме) соискателя – 30 дней		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных и типа носителя персональных данных		
2. Цель обработки: <u>обеспечение соблюдения трудового законодательства РФ</u>			
Категории данных	Персональные данные	Специальные персональные данные	Биометрические персональные данные

Перечень данных	<p>фамилия, имя, отчество; пол; гражданство; год рождения; месяц рождения; дата рождения; место рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; СНИЛС; ИНН; сведения об образовании; сведения о квалификации; сведения о профессиональной подготовке и повышении квалификации; семейное положение; доходы; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; профессия; должность; сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); отношение к воинской обязанности, сведения о воинском учете; иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства)</p>	сведения о состоянии здоровья; сведения о судимости	данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта персональных данных
Категории субъектов	Работники, Уволенные работники		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока трудового договора и периода после его завершения, необходимого для выполнения всех обязательств сторон		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе в составе личных дел – 50 лет		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных		

	и типа носителя персональных данных
3. Цель обработки: <u>подготовка, заключение и исполнение гражданско-правового договора</u>	
Категории данных	Персональные данные
Перечень данных	фамилия, имя, отчество; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; ИНН; СНИЛС; реквизиты банковской карты; номер расчетного счета; номер лицевого счета; иные персональные данные, предоставляемые физическими лицами, необходимые для заключения и исполнения договоров
Категории субъектов	Контрагенты, Представители контрагентов, Выгодоприобретатели по договорам
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет
Сроки обработки	В течение срока, необходимого для исполнения заключенного договора
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных и типа носителя персональных данных
4. Цель обработки: <u>обеспечение пропускного режима на территорию Оператора</u>	
Категории данных	Персональные данные
Перечень данных	фамилия, имя, отчество; данные документа, удостоверяющего личность
Категории субъектов	Посетители, Работники, Уволенные работники, Кандидаты на работу (соискатели), Контрагенты, Представители контрагентов, Выгодоприобретатели по договорам, Учащиеся, Законные представители учащихся
Способы обработки	Неавтоматизированная, внесение персональных данных в журнал учета посетителей
Сроки обработки	В течение срока, необходимого для ведения журнала учета посетителей
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных и типа носителя персональных данных

5. Цель обработки: <u>обеспечение соблюдения трудового законодательства РФ</u>			
Категории данных	Персональные данные		
Перечень данных	фамилия, имя, отчество; пол; гражданство; год рождения; месяц рождения; дата рождения; место рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; сведения об образовании; сведения о трудовой деятельности; иные персональные данные, предоставляемые родственниками работников в соответствии с требованиями трудового законодательства		
Категории субъектов	Родственники работников		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока трудового договора работника и периода после его завершения, необходимого для выполнения всех обязательств сторон		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе в составе личных дел – 50 лет		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных и типа носителя персональных данных		
6. Цель обработки: <u>обеспечение соблюдения законодательства РФ в сфере образования</u>			
Категории данных	Персональные данные	Специальные персональные данные	Биометрические персональные данные
Перечень данных	фамилия, имя, отчество; пол; гражданство; год рождения; месяц рождения; дата рождения; место рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона;	сведения о состоянии здоровья	данные изображения лица, полученные с помощью фото-видео устройств, позволяющие установить личность субъекта персональных данных

	адрес электронной почты; СНИЛС; сведения об образовании; иные персональные данные, предоставляемые Учащимися необходимые для обеспечения соблюдения законодательства РФ в сфере образования и/или заключения и исполнения договоров		
Категории субъектов	Учащиеся		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока обучения и периода после его завершения, необходимого для выполнения всех обязательств сторон		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных и типа носителя персональных данных		
7. Цель обработки: <u>обеспечение соблюдения законодательства РФ в сфере образования</u>			
Категории данных	Персональные данные		
Перечень данных	фамилия, имя, отчество; пол; год рождения; месяц рождения; дата рождения; данные документа, удостоверяющего личность; адрес регистрации; адрес места жительства; номер телефона; адрес электронной почты; иные персональные данные, предоставляемые Законными представителями учащихся необходимые для обеспечения соблюдения законодательства РФ в сфере образования и/или заключения и исполнения договоров		
Категории субъектов	Законные представители учащихся		
Способы обработки	Смешанная обработка, с передачей по внутренней сети юридического лица, без передачи по сети Интернет		
Сроки обработки	В течение срока обучения учащихся и периода после его завершения, необходимого для выполнения всех обязательств сторон		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные		
Порядок уничтожения	В соответствии с Регламентом уничтожения персональных данных в Учреждении в зависимости от способа обработки персональных данных		

III. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Правовые основания обработки персональных данных:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.2. Перечень нормативных правовых актов, локальных нормативных актов и иных документов во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора;
- устав Учреждения;
- договоры, заключаемые между Оператором и субъектами персональных данных;
- согласие субъектов персональных данных на обработку их персональных данных.

IV. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных:

4.1.1. Кандидаты на работу (соискатели) – для целей подбора персонала (соискателей) на вакантные должности оператора, обеспечение пропускного режима на территорию Оператора.

4.1.2. Работники, Уволенные работники – для целей обеспечения соблюдения трудового законодательства РФ и иных непосредственно связанных с ним отношений, обеспечение пропускного режима на территорию оператора.

4.1.3. Контрагенты, Представители контрагентов, Выгодоприобретатели по договорам – для целей подготовки, заключения и исполнения гражданско-правового договора, обеспечение пропускного режима на территорию Оператора:

4.1.4. Родственники работников – для целей обеспечения соблюдения трудового законодательства РФ и иных непосредственно связанных с ним отношений.

4.1.5. Учащиеся, Законные представители учащихся – для целей обеспечения соблюдения законодательства РФ в сфере образования, обеспечение пропускного режима на территорию Оператора.

4.2. Содержание и объем обрабатываемых персональных данных для каждой категории субъектов персональных данных указаны в разделе II настоящей Политики и должны соответствовать заявленным целям обработки, предусмотренным в этом разделе.

4.3. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.4. Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

4.5. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости за исключением случаев, предусмотренных законодательством РФ.

4.6. Трансграничная передача персональных данных субъектов персональных данных Оператором не осуществляется.

V. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

5.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

5.3. Оператор осуществляет обработку персональных данных для каждой цели их обработки следующими способами:

- неавтоматизированная обработка персональных данных;
- смешанная обработка персональных данных, с передачей по внутренней сети юридического лица, без передачи по сети Интернет.

5.4. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

5.5. Обработка персональных данных для каждой цели обработки, указанной в пункте 2.3 Политики, осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;
- внесения персональных данных в журналы, реестры и информационные системы Оператора;
- использования иных способов обработки персональных данных.

5.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 № 18.

5.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- определяет угрозы безопасности персональных данных при их обработке;
- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лицо, ответственное за организацию обработки персональных данных в Учреждении и за обеспечение безопасности персональных данных в информационных системах Оператора;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- организует работу с информационными системами, в которых обрабатываются персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;
- организует обучение работников Оператора, осуществляющих обработку персональных данных.

5.9. Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

5.9.1. Персональные данные на бумажных носителях хранятся в Учреждении в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 № 236)).

5.9.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

5.10. Оператор прекращает обработку персональных данных в следующих случаях:

- немедленно по требованию субъекта персональных данных обработку его персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- выявлен факт их неправомерной обработки. Срок – в течение трех рабочих дней с даты выявления;
- достигнута цель их обработки;

- истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.

5.11. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Оператор прекращает обработку этих данных, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

5.12. При обращении субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Оператором соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору необходимо направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока.

5.13. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

VI. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ, УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

6.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

- подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

6.4. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

- в течение 24 часов – уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемой вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом (первичное уведомление);

- в течение 72 часов – уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии) (дополнительное уведомление).

6.5. Взаимодействие оператора с Роскомнадзором в рамках ведения реестр учета инцидентов в области персональных данных осуществляется в виде направления первичного и дополнительного уведомления в соответствии с приказом Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

6.6. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Закона о персональных данных, производится

в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"».

6.7. Порядок уничтожения персональных данных Оператором.

6.7.1. Условия и сроки уничтожения персональных данных Оператором:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель – в течение не более 30 дней с даты достижения цели обработки;
- достижение максимальных сроков хранения документов, содержащих персональные данные, – в течение не более 30 дней;
- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, – в течение не более 7 рабочих дней со дня представления сведений субъектом персональных данных;
- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, – в течение не более 30 дней с даты поступления указанного отзыва;
- при невозможности обеспечить правомерность обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, – в течение не более 10 рабочих дней с даты выявления неправомерной обработки персональных данных;
- в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.7.2. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;
- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

6.7.3. Уничтожение персональных данных осуществляет комиссия, созданная приказом руководителя Учреждения.

6.7.4. Способы уничтожения персональных данных устанавливаются в локальных нормативных актах Оператора.

6.7.5. Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями, установленными приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

**РЕГЛАМЕНТ
ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ
ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ НАРУШЕНИЯ ФЕДЕРАЛЬНОГО
ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»**

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Регламент оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (далее – Регламент) определяет единый и обязательный порядок и методику оценки вреда, который может быть причинён субъекту персональных в случае нарушения требований Федерального закона «О персональных данных» в МБДОУ «Детский сад № 8» (далее – Оператор, Организация).

Настоящий Регламент принят в целях обеспечения соответствия деятельности Оператора требованиям Федерального закона «О персональных данных».

Настоящий документ обязаны знать и использовать в работе члены комиссии по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

3. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка возможного вреда субъекту персональных данных осуществляется комиссией по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», назначенной приказом руководителя Организации, в соответствии с методикой, описанной в разделе 4 настоящего Регламента.

По результатам оценки уровня возможного вреда субъекту персональных данных оформляется акт оценки возможного вреда субъекту персональных данных.

Допускается оформление одного акта на несколько категорий субъектов персональных данных.

4. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекту персональных данных может быть причинён вред в форме:

а) убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

б) морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Оценка степени вреда, который может быть причинен субъекту персональных данных осуществляется в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"».

Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных.

Высокая степень вреда устанавливается в случаях:

- обработки Оператором сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

- обработки Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

- обработки Оператором персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;

- обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

- поручения иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;

- сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

Средняя степень вреда устанавливается в случаях:

- распространения персональных данных на официальном сайте Оператора в сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;

- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;

- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;

- получения согласия на обработку персональных данных посредством реализации на официальном сайте в сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;

- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

5. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ ВРЕДА

Результаты оценки вреда оформляются актом оценки вреда.

Акт оценки вреда должен содержать:

- а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;
- б) дату издания акта оценки вреда;

в) дату проведения оценки вреда;

г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;

д) степень вреда, которая может быть причинена субъекту персональных данных, определенная в соответствии с методикой оценки вреда, указанной в разделе 4 настоящего Регламента.

Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с методикой оценки вреда могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

6. ПЕРЕСМОТР РЕГЛАМЕНТА

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных Организации.

ПРИЛОЖЕНИЕ 2

РЕГЛАМЕНТ ПРОВЕДЕНИЯ ВНУТРЕННЕГО РАССЛЕДОВАНИЯ В СВЯЗИ С ПРОИЗОШЕДШИМ ИНЦИДЕНТОМ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет единый и обязательный порядок проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, в МБДОУ «Детский сад № 8» (далее – Оператор, Организация).

3. ПРОВЕДЕНИЕ ВНУТРЕННЕГО РАССЛЕДОВАНИЯ ИНЦИДЕНТА

Проведение внутреннего расследования и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- халатность и несоблюдение требований по обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования возлагается приказом руководителя на комиссию в области персональных данных (далее – Комиссия). Комиссия должна приступить к работе по расследованию не позднее следующего дня после даты выявления нарушения.

Общая продолжительность внутреннего расследования не должна превышать 72 часов с момента выявления нарушения или инцидента в области персональных данных.

4. ПРАВА И ОБЯЗАННОСТИ КОМИССИИ

Права и обязанности Комиссии:

- опрос работников, допустивших нарушение конфиденциальности информации, а также лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента в области персональных данных;
- проведение осмотров объектов и предметов, которые могут иметь отношение к факту нарушения;
- привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом руководителя о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (актами, справками и т. п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии (не менее чем за двумя подписями).

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения руководителя Оператора.

Для организованного и оперативного проведения внутреннего расследования Администратор безопасности разрабатывает версии причин и составляет план проведения необходимых мероприятий по каждой из этих версий. В ходе расследования могут выдвигаться и отрабатываться дополнительные версии, в этом случае план действий уточняется.

Одновременно с проведением внутреннего расследования, руководитель Оператора может поручить Комиссии определить актуальность утраченной (разглашенной) конфиденциальной информации, оценить вред, который возможно был причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", а также определить (подсчитать) ущерб (убытки) по расследуемому факту. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

5. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ РАССЛЕДОВАНИЯ

По окончании внутреннего расследования Комиссия представляет руководителю Оператора заключение, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;

- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- степень вреда, который был причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т.д.).

К заключению прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба (убытков), оценке вреда.

Заключение должно быть подписано всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Заключение по результатам расследования подлежит утверждению руководителя Оператора.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель, имеют право знакомиться с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с заключением по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях лица признаков административного правонарушения или уголовного преступления руководитель обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством Российской Федерации.

В соответствии с Трудовым кодексом возмещение ущерба проводится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

Первый экземпляр заключения с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дело о внутренних расследованиях вносится в номенклатуру дел Оператора.

**РЕГЛАМЕНТ
ПО ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ И РЕАГИРОВАНИЮ
НА ИНЦИДЕНТЫ, СВЯЗАННЫЕ С НЕПРАВОМЕРНОЙ ИЛИ СЛУЧАЙНОЙ
ПЕРЕДАЧЕЙ (ПРЕДОСТАВЛЕНИЕМ, РАСПРОСТРАНЕНИЕМ, ДОСТУПОМ)
ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет единый и обязательный порядок реагирования на инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, а также порядок проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в МБДОУ «Детский сад № 8» (далее – Оператор, Организация).

3. ОПРЕДЕЛЕНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСПДН

К инцидентам, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных (далее – инциденты информационной безопасности, инциденты ИБ) относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или) защиты ПДн;
- несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты и обработки персональных данных;
- заражение вредоносными программами информационных систем персональных данных,
- в случае если эти события привели к неправомерной или случайной передаче (предоставлению, распространению, доступу) персональных данных, повлекшей нарушение прав субъектов персональных данных.

К инцидентам информационной безопасности в ИСПДн также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн с нарушением установленного времени доступа;
- сеансы работы Пользователей ИСПДн, срок действия полномочий которых истек либо в состав полномочий которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
- совершение попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты ПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для наступления случаев, описанных выше.

4. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

– 4.1 ОПОВЕЩЕНИЕ ОБ ИНЦИДЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Последовательность действий работника Оператора в случае выявления инцидента ИБ:

- прекратить работу с ресурсом, в котором выявлен инцидент ИБ;
- оповестить непосредственного руководителя о факте выявления инцидента ИБ;
- непосредственный руководитель работника должен оповестить Администратора безопасности персональных данных о факте выявления инцидента;
- после извещения ответственных сотрудников по их решению представить всю необходимую информацию.

Администратор безопасности персональных данных проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ.

– 4.2 МЕРОПРИЯТИЯ ПРИ НАСТУПЛЕНИИ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СТАВШЕГО ПРИЧИНОЙ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ ДЛЯ СУБЪЕКТА ПДН

В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов ПДн, персональные данные этих субъектов необходимо немедленно блокировать до устранения причин, повлекших наступление инцидента ИБ и его последствий. Решение о блокировании персональных данных принимает Администратор безопасности персональных данных. Для этой цели Администратор безопасности персональных данных блокирует персональные данные.

Менеджер обработки ПДн уведомляет субъекта о блокировании его персональных данных.

Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ.

Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Менеджер обработки ПДн и Администратор безопасности персональных данных обеспечивают немедленное уничтожение персональных данных.

Менеджер обработки ПДн оповещает субъекта ПДн о прекращении и уничтожении его персональных данных.

– 4.3 УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на Администратора безопасности персональных данных. Не позднее 24 часов с момента наступления инцидента Администратор безопасности составляет План устранения последствий и причин наступления инцидента информационной безопасности. В данный план целесообразно включить:

- общую информацию о произошедшем инциденте;
- анализ ситуации, оперативные контрмеры, которые можно применить для локализации инцидента;

- определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента;
- определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента.

– **4.4 ПРОВЕДЕНИЕ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- халатность и несоблюдение требований по обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Внутреннее расследование проводится в соответствии с Регламентом проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных.

Результаты внутреннего расследования оформляются в виде заключения.

Заключение с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле.

Дело о внутренних расследованиях вносится в номенклатуру дел Оператора.

– **4.5 ПРЕВЕНТИВНЫЕ МЕРЫ ПО НЕДОПУЩЕНИЮ ПОВТОРНОГО ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение в зависимости от произошедшего инцидента ИБ включают в себя:

- мониторинг событий в информационной системе персональных данных;
- восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе персональных данных;
- контроль над действиями системных администраторов;
- проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;
- ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных;
- пересмотр организационно-распорядительной документации, устанавливающей правила обработки и обеспечения безопасности при работе с персональными данными.

5. ОЦЕНКА ЭФФЕКТИВНОСТИ РЕАЛИЗОВАННЫХ МЕР В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится комиссией по проведению в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных Оператора организуется и проводится администратором безопасности информационных систем персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер и контроль за выполнением требований защиты персональных данных в информационных системах персональных данных проводится администратором безопасности информационных систем персональных данных и менеджером обработки персональных данных не реже 1 раза в 12 месяцев. Итоги проведенных мероприятий по проверке состояния защиты персональных данных вносятся в План внутренних проверок состояния защиты персональных данных (Приложение 1).

6. УВЕДОМЛЕНИЕ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБ ИНЦИДЕНТЕ

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом (первичное уведомление);

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии) (дополнительное уведомление).

Взаимодействие Оператора с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в рамках ведения реестра учета инцидентов в области персональных данных осуществляется в рамках приказа Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

Первичное уведомление должно содержать:

1) Сведения:

- о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – скомпрометированная база данных), количество содержащихся в ней записей). Дополнительно оператор может представить информацию об актуальности

скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

- о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

- о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона «О персональных данных»);

- о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых оператором организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона «О персональных данных»);

- о лице, уполномоченном оператором на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

2) Данные оператора, направившего уведомление:

- фамилию, имя и отчество (при наличии) гражданина, индивидуального предпринимателя;

- полное и сокращенное (при наличии) наименование юридического лица;

- идентификационный номер налогоплательщика юридического лица, индивидуального предпринимателя, физического лица;

- адрес регистрации по месту жительства (пребывания) физического лица, индивидуального предпринимателя;

- адрес юридического лица в пределах места нахождения юридического лица;

- адрес электронной почты (при наличии).

3) Иные сведения и материалы, находящиеся в распоряжении оператора, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

Дополнительное уведомление должно содержать сведения:

- о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

- о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица оператора с указанием должности (если причиной инцидента стали действия сотрудника оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении оператора).

В случае если оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Уведомление в форме электронного документа направляется оператором посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети "Интернет" (далее – Портал персональных данных), после прохождения процедуры идентификации и аутентификации посредством федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее – ЕСИА) и подписывается электронной подписью.

Оператору с момента поступления уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления.

При направлении дополнительного уведомления посредством Портала персональных данных оператор должен указать номер и ключ уведомления.

В случае направления оператором неполных или некорректных сведений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, не позднее трех рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос оператору о представлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

Недостающие сведения и (или) пояснения относительно некорректности представленных в уведомлении сведений предоставляются оператором в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение трех рабочих дней со дня получения запроса.

6. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ДОКУМЕНТЫ ОПЕРАТОРА

Пересмотр положений настоящего и иных локальных документов Оператора, касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности персональных данных и Менеджер обработки ПДн.

Внесение изменений производится на основании соответствующего приказа руководителя Оператора.

– ПЛАН ВНУТРЕННИХ ПРОВЕРОК

– СОСТОЯНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование мероприятий	Срок/периодичность	Ответственный/исполнитель
Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных	1 раз в 12 месяцев	Менеджер обработки ПДн
Оценка эффективности реализованных в рамках системы защиты персональных данных мер	1 раз в 12 месяцев	Администратор безопасности ИСПДн
<...>		

ПРИЛОЖЕНИЕ 4

**РЕГЛАМЕНТ
РЕАГИРОВАНИЯ ОПЕРАТОРА НА ЗАПРОСЫ/ОБРАЩЕНИЯ
УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ
ПЕРСОНАЛЬНЫХ ДАННЫХ, СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ
ПРЕДСТАВИТЕЛЕЙ ПО ПОВОДУ НЕТОЧНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ,
НЕПРАВОМЕРНОСТИ ИХ ОБРАБОТКИ, ОТЗЫВА СОГЛАСИЯ И ДОСТУПА
СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ К СВОИМ ПЕРСОНАЛЬНЫМ
ДАННЫМ**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент реагирования Оператора на запросы/обращения уполномоченного органа по защите прав субъектов персональных данных, субъектов персональных данных и их представителей по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным (далее – Регламент) определяет последовательность действий при рассмотрении запросов/обращений уполномоченного органа по защите прав субъектов персональных данных, субъектов персональных данных или их представителей, поданных в соответствии с частью 1 статьи 14 Федерального закона «О персональных данных», правила ведения делопроизводства по Запросам, поступающим в адрес МБДОУ «Детский сад № 8» (далее – Оператор, Организация), а также осуществление контроля за соблюдением Регламента.

1.2. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

1.3. Запрос субъекта персональных данных (далее – Запрос) – требование субъекта персональных данных и/или их представителей от Оператора уточнения персональных

данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

1.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.5. Рассмотрение Запросов в Организации, являющейся в соответствии со статьей 3 Федерального закона «О персональных данных» Оператором, осуществляющим обработку персональных данных, выполняется с соблюдением прав субъектов персональных данных или их представителей и в соответствии с обязанностями оператора, определенными Федеральным законом «О персональных данных».

2. ПРИЁМ И РЕГИСТРАЦИЯ ЗАПРОСОВ

2.1. Запросы могут быть доставлены лично, через представителей, почтовым отправлением, по электронным каналам связи в форме электронного документа, подписанного электронной подписью, в соответствии с законодательством Российской Федерации.

2.2. Запросы в Оператора, поступающие непосредственно от субъектов персональных данных (далее – субъект), принимаются и регистрируются в приемной руководителя Организации.

2.3. Если к Запросу прилагаются подлинные документы, удостоверяющие личность (паспорт, свидетельство, удостоверение и другие документы), с них снимаются копии, оригиналы возвращаются непосредственно субъекту или отправляются заказным письмом по указанному в Запросе адресу.

2.4. Работник Оператора, при прочтении Запроса проверяет правильность адресования Запроса, проверяет историю Запросов субъекта на повторность.

2.5. В Запросах, поступивших повторно и удовлетворяющих требованиям частей 4 и 5 статьи 14 Федерального закона «О персональных данных», делается отметка о повторном поступлении Запроса, и к нему приобщаются копии материалов предыдущих Запросов. Оператор вправе отказать субъекту персональных данных или его представителю в рассмотрении повторного Запроса, не соответствующего требованиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона «О персональных данных». Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного Запроса лежит на Операторе.

2.6. Работник Оператора, заносит необходимую информацию о Запросе в журнал учета обращений субъектов персональных данных.

2.7. Регистрация Запросов производится путем присвоения порядкового номера каждому поступившему Запросу в течение трех календарных дней с даты их поступления, информация о запросе вносится в журнал (типовая форма журнала приведена в Приложении 1 к настоящему Регламенту). На лицевой стороне первого листа в правом нижнем углу письменного Запроса проставляется регистрационный штамп. В случае если

место, предназначенное для регистрационного штампа, занято текстом, штамп может быть проставлен в ином месте, обеспечивающем его прочтение.

2.8. Запрос, ошибочно поступивший в адрес Оператора, направляется исполнителем по указанному в Запросе адресу с сопроводительным письмом с уведомлением субъекта персональных данных или его представителя, направившего Запрос, о переадресации Запроса.

3. НАПРАВЛЕНИЕ ЗАПРОСА НА РАССМОТРЕНИЕ

3.1. После регистрации, в тот же день, Запрос, поступивший в адрес Оператора, вместе с карточкой передается руководителю Организации, для рассмотрения, определения исполнителя (ответственное лицо) и формирования поручения по Запросу.

3.2. Срок для определения исполнителей и дачи поручений по Запросу не может превышать пять календарных дней, которые входят в основной (десять рабочих дней) срок рассмотрения Запроса со дня его регистрации.

3.3. В случае если Запрос, поступивший в адрес Оператора, содержит требование уточнить персональные данные, заблокировать их или уничтожить в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, руководитель в тот же день определяет исполнителей и дает поручение осуществить блокирование неправомерно обрабатываемых либо неточных персональных данных, относящихся к этому субъекту персональных данных с даты получения указанного Запроса на период проверки.

3.4. В поручении указываются фамилии, инициалы исполнителей, содержание поручения (при необходимости), срок исполнения, дата и подпись.

4. ПОРЯДОК РАССМОТРЕНИЯ ЗАПРОСА

4.1. Ответственное лицо при рассмотрении Запроса обеспечивает объективное, всестороннее и своевременное рассмотрение Запроса, запрашивает необходимые для рассмотрения Запроса документы и материалы у работников Организации, по компетенции.

4.2. Запрос рассматривается не более десяти рабочих дней со дня его получения, если статьями 20, 21 Федерального закона «О персональных данных» не установлен более короткий срок рассмотрения Запроса.

4.3. В установленный срок (десять рабочих дней) входит время на визирование (определение исполнителей и нанесение поручений), рассмотрение Запроса по существу, подготовку текста ответа, его возможное согласование, подписание и направление ответа субъекту персональных данных.

4.4. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.5. В случае обращения субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных Оператор обязан в срок, не превышающий десяти рабочих дней с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных».

4.6. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных

мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.7. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

4.8. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5. ОФОРМЛЕНИЕ ОТВЕТА НА ЗАПРОСЫ

5.1. Ответы на Запросы, поступившие в адрес Оператора, подписываются руководителем Организации или его заместителем (в случае официального отсутствия).

5.2. Подготовку ответа обеспечивает руководитель структурного подразделения Организации, в соответствии с поручением по Запросу. В случае если в поручении указано несколько исполнителей, ответственным исполнителем считается лицо, указанное первым в поручении по Запросу. Ответ на Запрос готовит основной исполнитель, указанный в поручении первым, при этом другие исполнители визируют данный ответ.

5.3. Ответ на Запрос, поступивший по информационным системам общего пользования, направляется по почтовому адресу, указанному в Запросе.

5.4. Текст ответа должен излагаться четко, последовательно, кратко, исчерпывающе давать пояснения на все поставленные вопросы.

5.5. Запрос считается исполненным, если по существу поставленных вопросов субъекту персональных данных или его представителю в представлении сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», или приняты меры, предусмотренные частью 3 статьи 20 и частями 1-3 статьи 21 Федерального закона «О персональных данных».

5.6. Оператор предоставляет сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

5.7. Ответы на письменные Запросы оформляются в соответствии с порядком, установленным Инструкцией по делопроизводству в Организации, и должны содержать дату и регистрационный номер документа, фамилию и инициалы гражданина, его почтовый адрес, текст документа (ответ на Запрос), наименование должности лица, подписавшего документ, его инициалы, фамилию, подпись, а также инициалы, фамилию и номер телефона исполнителя.

6. КОНТРОЛЬ СОБЛЮДЕНИЯ РЕГЛАМЕНТА

6.1. Контроль соблюдения Регламента возлагается на заместителя руководителя Организации ответственного за организацию обработки персональных данных в Организации.

6.2. Организация делопроизводства по Запросам и контролю за своевременным, объективным и полным рассмотрением Запросов, поступивших в адрес Оператора, осуществляется работником ответственным за прием и регистрацию входящих документов в Организации.

ПРИЛОЖЕНИЕ 5

РЕГЛАМЕНТ УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Регламент уничтожения персональных данных (далее – Регламент) определяет единый и обязательный порядок, условия и способы уничтожения персональных данных субъектов персональных данных, которые обрабатываются в МБДОУ «Детский сад № 8» (далее – Оператор, Организация), а также устанавливает формы подтверждения уничтожения персональных данных.

2.2. Настоящий Регламент принят в целях обеспечения защиты прав и свобод обучающихся и работников при обработке их персональных данных и обеспечения соответствия деятельности Оператора требованиям Федерального закона «О персональных данных».

2.3. Настоящий Регламент разработан на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» и других нормативных правовых актов.

2.4. Настоящий Регламент обязаны знать и использовать в работе члены комиссии по уничтожению персональных данных.

3. ПОРЯДОК УНИЧТОЖЕНИЯ НОСИТЕЛЕЙ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- подтверждаться юридически, в частности, оформлением соответствующих документов, установленных законодательством;
- должно проводиться комиссией по уничтожению персональных данных, утвержденной приказом директора Организации (далее – Комиссия);
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3.2. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются в специально отведенном для этих целей помещении Комиссией.

3.4. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных либо утраты необходимости в их достижении, а также в случае, если истек срок их хранения.

3.5. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.6. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.7. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению и актах об уничтожении персональных данных субъектов персональных данных, исправления не допускаются.

3.8. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.9. По окончании сверки акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается руководителем Организации.

3.10. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются ответственному за уничтожение документов в помещение отдела кадров.

3.11. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

3.12. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.13. Уничтожение персональных данных, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием shreddera (уничтожителя документов), установленного в помещении отдела кадров, либо документы передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);

- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустраняемого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;

- подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске средств автоматизации или в базах данных ИСПДн, удаляются средствами операционной системы компьютера и/или с использованием специального программного обеспечения;

- в случае допустимости повторного использования носителя флэш, CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

– **4. ПОРЯДОК ПОДТВЕРЖДЕНИЯ УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. В случае если обработка персональных данных осуществляется Оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

4.2. В случае если обработка персональных данных осуществляется Оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в ИСПДн (далее – выгрузка из журнала).

4.3. Акт об уничтожении персональных данных составляется и подписывается всеми членами Комиссии и утверждается руководителем Организации.

4.4. Акт об уничтожении персональных данных должен содержать:

а) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес Оператора;

б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению Оператора (если обработка была поручена такому (таким) лицу (лицам));

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

4.5. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г" пункта 4.4 настоящего Регламента.

4.6. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

4.7. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 5 настоящих Требований, недостающие сведения вносятся в акт об уничтожении персональных данных.

4.8.. В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала.

4.9. Факт уничтожения персональных данных субъектов персональных данных, фиксируется в журнале регистрации уничтожения ПДн субъектов ПДн. Данный документ является документом конфиденциального характера и вместе с актами о выделении документов, содержащих персональные данные субъектов персональных данных, актами об уничтожении персональных данных и выгрузками из журнала регистрации событий хранится в помещении отдела кадров в течение 3 лет с момента уничтожения персональных данных. По истечении срока указанные документы передаются в архив Организации на хранение.

6. ПЕРЕСМОТР РЕГЛАМЕНТА

Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных Организации.

ПРИЛОЖЕНИЕ 6

УТВЕРЖДАЮ

(руководитель организации)

(подпись) (расшифровка подписи)

"__" _____ 20__ г.

Акт № _____

**оценки вреда, который может быть причинен субъектам персональных данных
в случае нарушения Федерального закона «О персональных данных»**

г. _____

"__" _____ 20__ г.

Комиссия, уполномоченная

(наименование (юридического лица) или фамилия, имя, отчество (при наличии) (физического лица)

и адрес оператора)

в составе председателя

(фамилия, имя, отчество (при наличии), должность)

И ЧЛЕНОВ

(фамилия, имя, отчество (при наличии), должность)

(фамилия, имя, отчество (при наличии), должность)

наделенная полномочиями в соответствии с

(реквизиты документа о создании комиссии и наделении ее полномочиями)

составила настоящий акт о нижеследующем:

Комиссией в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"»

(дата проведения оценки вреда)

осуществлена оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

и определена степень вреда, который может быть причинен субъекту персональных данных, –

(укажите степень вреда, который может быть причинен субъекту персональных данных: высокая, средняя или низкая)

Обоснование:

(укажите обоснование выбора комиссией степени вреда)

Председатель комиссии:

(должность (при наличии) председателя комиссии)

(подпись председателя комиссии)

(расшифровка подписи председателя комиссии)

" __ " _____ 20__ Г.

Члены комиссии:

(должность (при наличии) члена комиссии)

(подпись члена комиссии)

(расшифровка подписи члена комиссии)

" __ " _____ 20__ Г.

(должность (при наличии) члена комиссии)

(подпись члена комиссии)

(расшифровка подписи члена комиссии)

" __ " _____ 20__ Г.

ПРИЛОЖЕНИЕ 7
УТВЕРЖДАЮ

(руководитель организации)

(подпись) (расшифровка подписи)

"__" "_____" 20__ г.

Акт № _____

об уничтожении персональных данных

г. _____

"__" "_____" 20__ г.

Комиссия, уполномоченная

(наименование (юридического лица) или фамилия, имя, отчество (при наличии) (физического лица))

и адрес оператора)

и/или

(наименование (юридического лица) или фамилия, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего

(осуществляющих) обработку ПДн субъекта (субъектов) ПДн по поручению оператора (если обработка была поручена такому (таким) лицу (лицам))

в составе председателя

(фамилия, имя, отчество (при наличии), должность)

и членов

(фамилия, имя, отчество (при наличии), должность)

(фамилия, имя, отчество (при наличии), должность)

наделенная полномочиями в соответствии с

(реквизиты документа о создании комиссии и наделении ее полномочиями)

составила настоящий акт о нижеследующем:

Комиссией в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ

(дата, время и место уничтожения ПДн субъекта (субъектов) ПДн)

было произведено уничтожение персональных данных

(перечень категорий ПДн субъекта (субъектов) ПДн)

принадлежащих:

(фамилия, имя, отчество (при наличии) субъекта (субъектов) или иная информация, относящаяся к определенному (определенным)

физическому (физическим) лицу (лицам), чьи ПДн были уничтожены)

Причина уничтожения персональных данных:

(причина и/или правовое (правовые) основание (основания) уничтожения ПДн)

Персональные данные находились:

(наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) ПДн субъекта (субъектов) ПДн,

с указанием количества листов в отношении каждого материального носителя (в случае обработки ПДн без использования средств автоматизации))

и/или

(наименование информационной (информационных) системы (систем) ПДн, из которой (которых) были уничтожены ПДн

субъекта (субъектов) ПДн (в случае обработки ПДн с использованием средств автоматизации))

Уничтожение материальных носителей персональных данных осуществлено путем:

(способ уничтожения носителей ПДн: измельчение, шредирование, разрезание, сжигание, механическое уничтожение и т.п.)

Уничтожение персональных данных в ИСПДн осуществлено путем:

(способ уничтожения ПДн в ИСПДн: стирание на носителе, уничтожение с помощью специального ПО, механическое уничтожение т.п.)

Председатель комиссии:

(должность (при наличии) председателя комиссии)
" __ " _____ 20__ Г.

(подпись председателя комиссии)

(расшифровка подписи председателя комиссии)

Члены комиссии:

(должность (при наличии) члена комиссии)
" __ " _____ 20__ Г.

(подпись члена комиссии)

(расшифровка подписи члена комиссии)

(должность (при наличии) члена комиссии)
" __ " _____ 20__ Г.

(подпись члена комиссии)

(расшифровка подписи члена комиссии)

(наименование организации)

ЖУРНАЛ учета обращений субъектов персональных данных и их законных представителей

Том _____
Начат « ____ » _____ 20__ г.
Окончен « ____ » _____ 20__ г.
Всего _____ (_____) листов

Срок хранения _____
Хранить до « ____ » _____ 20__ г.

Ответственные за ведение журнала

№ п/п	Период ведения		Фамилия, имя, отчество (при наличии) ответственного лица	Должность	Действует на основании приказа (распоряжения)	Подпись ответственного лица
	с	по				
1	2	3	4	5	6	7

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи или отказа в предоставлении информации	Подпись ответственного	Примечание
1	2	3	4	5	6	7

Лицо, ответственное за ведение журнала на дату его окончания

_____ (должность)

_____ (подпись)

(наименование организации)

ЖУРНАЛ регистрации событий в информационной системе персональных данных

Том _____
 Начат « ____ » _____ 20__ г.
 Окончен « ____ » _____ 20__ г.
 Всего _____ (_____) листов

Срок хранения _____
 Хранить до « ____ » _____ 20__ г.

Ответственные за ведение журнала

№ п/п	Период ведения		Фамилия, имя, отчество (при наличии) ответственного лица	Должность	Действует на основании приказа (распоряжения)	Подпись ответственного лица
	с	по				
1	2	3	4	5	6	7

№ п/п	Дата уничтожения ПДн субъекта (субъектов) ПДн	Ф. И. О. субъекта (субъектов) ПДн, чьи ПДн были уничтожены	Перечень категорий уничтоженных ПДн субъекта (субъектов) ПДн	Наименование ИСПДн, из которой были уничтожены ПДн	Причина уничтожения ПДн	Номер, дата акта об уничтожении ПДн (при наличии)	Примечание
1	2	3	4	5	6	7	8

Лицо, ответственное за ведение журнала на дату его окончания

_____ (должность)

_____ (подпись)

(наименование организации)

ЖУРНАЛ регистрации уничтожения персональных данных

Том _____
Начат «___» _____ 20__ г.
Окончен «___» _____ 20__ г.
Всего _____ (_____) листов

Срок хранения _____
Хранить до «___» _____ 20__ г.

Ответственные за ведение журнала

№ п/п	Период ведения		Фамилия, имя, отчество (при наличии) ответственного лица	Должность	Действует на основании приказа (распоряжения)	Подпись ответственного лица
	с	по				
1	2	3	4	5	6	7

№ п/п	Дата уничтожения ПДн	Ф. И. О. работника (субъекта ПДн), ПДн которого были уничтожены	Перечень категорий ПДн, которые были уничтожены	Наименование носителя ПДн (ИСПДн)	Способ уничтожения ПДн	Причина уничтожения ПДн	Номер, дата акта об уничтожении ПДн	Ф. И. О. и подпись сотрудника, который осуществил уничтожение ПДн
1	2	3	4	5	6	7	8	9

Лицо, ответственное за ведение журнала на дату его окончания

_____ (должность)

_____ (подпись)